Ciphers and Number Theory 2

1. Encode the message `one of our agents has defected` using a Vigenère cipher with keyword SEAWEED.

2. Decode the message `UTUQO XFMJA DAUCW NTFEU PTWIX` using a Vigenère cipher with keyword ALPHABET.

3. Encode the message `call home at once for more instructions` using a Playfair cipher with keyword APRICOT.

4. Decode the message `QKRMB OQONC UVROT SNVNV RWCML KUZGB` using a Playfair cipher with keyword SUBMARINE.

5. Suppose that you receive three messages, of 10,000 letters each, with one encoded using a permutation cipher, one using a monoalphabetic substitution cipher, and one using a Playfair cipher. On analysing the messages you find the following statistics:

   (a) Message 1 contains the letter M 13% of the time, the letter T 9% of the time, and the letters U, A, S, W 7% of the time, with the remaining letters being less common.

   (b) Message 2 contains the letter E 12% of the time, the letter A 9% of the time, and the letters T, O, N, S 7% of the time, with the remaining letters being less common.

   (c) Message 3 contains the letters L, M 7% of the time, the letters P, E 6% of the time, and the letters A, G, R, S 5% of the time, with the other letters being less common.

   Which message is likely to use which cipher? What extra statistics would you want to have to help you crack the Playfair cipher? If each message contained only 50 letters would your conclusions be any different?

6. In a homophonic cipher, each letter can be encoded by several different symbols, depending on the frequency with which it occurs. Thus a rare letter like Z will only have one symbol, while a common letter like E will have many. When encoding a message, each letter is replaced by one of its corresponding symbols chosen at random.

   What advantage does this have over an ordinary monoalphabetic cipher?